**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION**

CENTRIPETAL NETWORKS, INC.,	
Plaintiff,	
vs.	Case No. 2:18-cv-00094-EWH-LRL
CISCO SYSTEMS, INC.,	
Defendant.	

**DEFENDANT CISCO SYSTEMS, INC.'S OPPOSITION TO PLAINTIFF'S MOTION
FOR ADDITIONAL AND AMENDED FINDINGS AND AMENDED JUDGMENT OR,
IN THE ALTERNATIVE, FOR A NEW TRIAL**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

Page(s)

INTRODUCTION

Defendant Cisco Systems, Inc. ("Cisco") respectfully opposes the motion of plaintiff Centripetal Networks, Inc. ("Centripetal") under Federal Rules of Civil Procedure 52 and 59.[1]

Centripetal compliments the Court for sailing through "most of the issues this case presents expertly" (Mem. 1), but in substance argues that the Court got basically everything wrong, including a technological distinction that "even laypeople understand" (Mem. 6). The Court did not make the series of blunders Centripetal asserts. Rather, the Court saw Centripetal's infringement case for what it was: an effort to broaden the patent claims to cover Cisco devices that do not practice what Centripetal's narrow claims recite.

Centripetal ventures that the Court was somehow precluded from considering claim construction. Mem. 1-2. But the Court did not reconstrue any previously-construed term, and it would not have mattered if it had. Contrary to Centripetal's unsupported assertions, the Court was not required to "treat some of the initial judge's findings and conclusions as binding" (Mem. 1) or to abide by "rulings made by Judge Morgan" (Mem. 3). As the Court repeatedly noted and Centripetal itself conceded, the Court may reconsider or clarify prior orders. Rule 63 Tr. 11:7-9, 322:23-323:22; *see also* Tr. 1646:11-1647:1, 1650:7-16 (Judge Morgan reconsidering *Markman* order during first trial); Rule 63 Tr. 323:18-19 (Centripetal's counsel: "You're right, Your Honor. Your Honor can consider [claim construction] and do what you will with it."); *see, e.g.*, *Exxon Corp. v. United States*, 931 F.2d 874, 878 (Fed. Cir. 1991); *In re Agent Orange Prod. Liab. Litig.*, 733 F.2d 10, 13 (2d Cir. 1984).

It is also too late for Centripetal to demand reopening the record to submit new

---

[1] "Mem." refers to the sealed version of Centripetal's supporting memorandum, Dkt. 791; "Tr." to the 2020 trial transcript; "Rule 63 Tr." to the 2023 Rule 63 hearing transcript; and "Op." to this Court's Memorandum Opinion and Order, Dkt. 780.

infringement theories. Cisco repeatedly presented the claim construction positions on which the Court relied, and Centripetal was able to (and did) address them. If Centripetal believed that Cisco's position warranted a new infringement theory (supported by new evidence or argument), it should have sought leave before the Rule 63 hearing (as the Court permitted, Rule 63 Tr. 10:4-12:2). That way, the necessary fact and expert record could have been developed and witnesses could have testified about the new theory, including allowing Cisco's experts to respond to the new infringement theory and argue invalidity based on that new theory. But Centripetal never sought leave before the Rule 63 hearing or at any time before the Court issued its decision. A party may not lie in wait to see how the Court rules, and then try to offer a new theory that it could have sought leave to present earlier but did not. Centripetal's motion should be denied.

ARGUMENT

A Rule 59(e) motion "may not be used … to raise arguments which could have been raised prior to the issuance of the judgment, nor may they be used to argue a case under a novel legal theory that the party had the ability to address in the first instance." *Pacific Ins. Co. v. American Nat'l Fire Ins. Co.*, 148 F.3d 396, 403 (4th Cir. 1998). Likewise, a Rule 52(b) motion should not be used "to introduce evidence that was available at trial but was not proffered, to relitigate old issues, to advance new theories, or to secure a rehearing on the merits." *Fontenot v. Mesa Petroleum Co.*, 791 F.2d 1207, 1219 (5th Cir. 1986).

I.   The '193 Patent

A.   The Court Did Not Construe A "Network" To Include "Just A Single Computer"

Contrary to Centripetal's lead argument (Mem. 6), the Court did not misunderstand the difference between a network and a computer. As Centripetal recognizes (*id.*), the Court described an exemplary first network that "consists of three computers" and a second network

2

that "consists of three sets of computers." Op. 11. This tracks the explanation of basic network architecture that both parties provided. Nor did the Court "assume that each network described in the claims contains just a single computer." Mem. 7. As the Court summarized, asserted claim 18 recites that the system "first 'receive[s] … a plurality of packets' from a computer in a 'first network.'" Op. 18 (quoting '193 Patent at 14:5-6). Centripetal does not dispute this recitation, which tracks the claim language. '193 Patent at 14:5-6 ("receive, from a computing device located in a first network, a plurality of packets").

As the Court explained, and Centripetal's motion does not deny, "[t]he disagreement between the parties comes down to whether the 'particular type of data transfer' claim limitation requires a system to drop some, but not all, packets sent between two different network destinations." Op. 24. The Court recognized that "in order to drop a packet, the claims require two conditions to be met: (1) the packets from the first network must be 'destined for [a] second network' and (2) the packets must meet rule criteria 'configured to prevent a particular type of data transfer from the first network to [the] second network.'" Op. 27 (quoting '193 Patent at 14:9-16). For both criteria to be given effect, "it is necessarily the case that only a portion of the packets destined for the second network meet the type of data transfer rule criteria specified by the second condition. Otherwise, the second condition would be rendered superfluous." Op. 25.

Centripetal does not challenge that understanding of the claims, which—as the Court noted—is consistent with the specification's disclosure of a filtering method with a "first stage" of determining whether a rule "'allows any communications between the resources identified'" and a "second stage" of "'determin[ing] if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources.'" Op. 19 (quoting '193 Patent at 8:45-52); Op. 25. It is also consistent with

3

Centripetal's arguments successfully defending the claims' validity before the PTAB (Op. 26)—

another point that Centripetal's motion does not acknowledge, much less deny.

The Court found, based on the testimony of both sides' experts, that the only "packet-

filtering rule" that Centripetal accused in Cisco's products—a "quarantine rule"—does not drop

only the subset of packets that both (1) are destined for the second network and additionally (2)

correspond to "a particular type of data transfer from the first network to the second network."

As the Court recognized (Op. 23) and Centripetal's motion does not address, when Judge

Morgan asked Centripetal's expert whether the quarantine rule would allow "some information

to go to [a separate network] and other information not to go to them that was generated from the

same source," the expert replied: "So the way typically the policies are instrumented is you

restrict *according to source and destination*. So you would say, well, I'm not going to let you

reach out to this other location, to this other network, right, and it will block sort of that -- it will

block the communication between you and that other network." Tr. 527:23-528:8

(Mitzenmacher);[2] *see also* Tr. 2399:8-2400:10 (Crovella). Centripetal's evidence at trial did not

map the second criterion (the "particular type of data transfer") to the accused quarantine rule.

Tr. 495:9-14 (Mitzenmacher) ("Based on the quarantine, if you've decided a user is a potential

threat, in particular there's an issue perhaps with exfiltration, you can instruct, you can create

rules that instruct the switches and routers to *permit or deny traffic going to or from certain*

places for that particular host."); Tr. 506:16-17 (Mitzenmacher) ("what this quarantine is set to

do, is to limit the network access of a particular user or group of users"); Tr. 2377:3-10

(Crovella); *see also* Dkt. 703 at 10 ("The Quarantine rule prevents particular types of data

---

[2] All emphasis is added unless otherwise noted.

4

transfers to or from potentially compromised computers—e.g., transfers involving networks with sensitive information—but allow transfers involving other networks, such as the Internet.").

The Court's analysis nowhere turned on "assum[ing] that each network described in the claims contains just a single computer" (Mem. 7); Centripetal cites no such language in the Court's opinion. Centripetal objects to the Court's statement that the claims require "filtration of a subset of packets sent between *computers* in two different networks" (Op. 24), but the word that Centripetal seizes on ("computers") is plural. Moreover, the fact that the claimed packets must originate from one or more "computers" is uncontroversial; claim 18 expressly recites that packets are received "from *a computing device* located in a first network." '193 patent at 14:5-6. And Centripetal itself used the word "computer" when describing the '193 patent. *E.g.*, Tr. 344:10-13 (Centripetal's examination of inventor Sean Moore: "Q. … after your *computer* has already been infected, [the '193 patent] is the technology that keeps that data from leaving the infected *computer*? A. Yes, that's one characterization."); Rule 63 Tr. 241:4-6 (Centripetal's closing: "the reason that the patent explained that you want to do this, is that if I am going to shut down a *computer* completely, it is very, very inefficient"). Centripetal's expert Dr. Mitzenmacher testified that the claimed packet traffic "might be coming to an endpoint or might be going out from an endpoint," and clarified that "it might be coming from your *computer* or going to your *computer*." Tr. 467:6-8; *see also* Rule 63 Tr. 41:12-17 (Medvidovic Tutorial) ("[O]n the right-hand side, we have an *end-user laptop*, and this skull and bones is indicating that there is something malicious happening on the *laptop*, and some information of yours that may be something you wish to protect in some way is getting exfiltrated and sent out into the open world.") The Court's contextual statement that a transmission of packets between two networks begins and ends at "computers in two different networks" reflects both parties'

5

explanation of how network communications work; it did not alter the claim scope any more than Centripetal's use of "computer" or "laptop" did.

B. Centripetal's New Infringement Theory Is Forfeited And Unsupported

Centripetal's claim construction discussion includes a single paragraph attempting to advance a new infringement contention under what it calls "the correct construction." Mem. 8. Centripetal's new theory is forfeited and unsupported.

Centripetal now argues that the claims' second packet-filtering rule criterion ("particular type of data transfer") could be met by an implementation that blocks **all** packets from one or more quarantined computers destined to the second network. Mem. 8. Centripetal's post-trial infringement theory is, apparently, that all packets from a quarantined computer are "a particular subset of data transfers from the first network to the second network" if other non-quarantined computers can send packets to the second network. Mem. 8. No such infringement theory was presented at trial, nor did Centripetal point to any expert testimony supporting such a theory when questioned at the Rule 63 Hearing.[3] The reason why is abundantly clear. Centripetal's

---

[3] *See, e.g.*, Tr. 489:17-491:2, 491:7-14, 495:4-14, 496:12-498:14, 501:9-502:10, 510:18-513:2, 519:2-521:2, 527:1-17, 527:23-528:8, 550:16-25, 869:1-12, 870:3-17 (Mitzenmacher) (testifying regarding "particular type of data transfer" limitation, but nowhere suggesting that all transfers from quarantined computers destined for a second network meet that rule criterion merely by virtue of being a subset of transfers from quarantined and non-quarantined computers to the second network); Tr. 3262:13-3269:18 (same for Centripetal's closing); Rule 63 Tr. 251:14-252:18, 262:23-263:12, 265:5-15, 268:5-269:20, 271:4-272:5, 273:12-274:8 (Centripetal's Rule 63 argument, including responding to Court's questions about trial testimony regarding this limitation); Dkt. 478-1 at 2-3 (Centripetal's post-trial Proposed Findings of Fact, acknowledging the quarantine rule was the accused "packet-filtering rule" but not expressly identifying any "particular type of data transfer"); *see also* Dkt. 703 at 10 (Centripetal's Rule 63 Trial Brief, acknowledging the same and equating "a particular type of data transfer" with "transfers involving networks with sensitive information"); Dkt. 725 at 35-36(¶¶153-160) (Centripetal's Rule 63 Proposed Findings of Fact, acknowledging the same but nowhere suggesting that the accused quarantine rule met the "particular type of data transfer" limitation under Centripetal's new infringement theory).

expert mapped the claimed "packet-filtering rules" only to Cisco's quarantine rule—a rule that is indisputably only applied to packets from quarantined computers and operates to block or allow all such packets based solely on their destination. Tr. 791:17-792:24, 869:1-12 (Mitzenmacher); Tr. 2385:23-2386:10, 2423:19-2424:15 (Crovella). Centripetal's post-trial infringement theory thus fails for the same reason as its only trial infringement theory failed: the accused quarantine rule, in its operation, blocks or allows all packets to which it is applied based solely on their destination, not additionally by "particular type of data transfer." *See also* Tr. 2386:12-2387:13 (Crovella); Tr. 527:23-528:8 (Mitzenmacher).

Indeed, when the Court asked Centripetal's counsel to identify "types of data transfers," Centripetal did not suggest that all packets destined for the second network from a quarantined computer in the first network would qualify as such a "subset." Rather, Centripetal sought to collapse the second rule criterion with the first rule criterion ("destined for the second network"), as it has throughout the case. Rule 63 Tr. 258:24-259:1 ("So the way that I think about data transfer is I'm transferring data, as the claims are saying, from one network to another."), 260:5-9 ("[T]he type of data transfer from that network to another network is going to be one type. If I have a data transfer from a network to a third network, I think that is a different type of data transfer, because you have different protocols."). Having previously failed to present any evidence, argument, or proposed findings in support of its new infringement theory, Centripetal cannot do so now. *E.g.*, *Perrier-Bilbo v. United States*, 954 F.3d 413, 435-436 (1st Cir. 2020) ("theories and arguments presented for the first time in [a Rule 52(b) motion] are not properly before the district court" (citing cases)); *Bendix Corp. v. United States*, 600 F.2d 1364, 1369 (Ct. Cl. 1979) (per curiam) (litigant "abandoned" defenses on which it "proposed no findings and

made no argument"); *Twin Disc, Inc. v. United States*, 10 Ct. Cl. 713, 784 (1986) (arguments

waived where not asserted "in either its post-trial brief or post-trial proposed findings of fact").

Notably, were Centripetal allowed to change its infringement accusation to encompass

any system "that can allow other computers in the first network … to transfer packets to the

second network" while "block[ing] certain computers in the first network – namely those that

have been assigned a 'quarantine' SGT tag – from transferring packets to a second network"

(Mem. 8), it would require redoing the entire case as to the '193 patent. Centripetal offered no

expert testimony supporting such an accusation, nor did Centripetal seek leave to recall its

infringement expert to provide such testimony during the Rule 63 Hearing, which would have

afforded Cisco an opportunity to proffer its own expert testimony rebutting it. Cisco would also

need the opportunity to develop invalidity theories showing that its prior art TrustSec

technology, implemented on its prior art routers and switches, plainly employed such a simple

network-access scheme. *See 01 Communique Lab., Inc. v. Citrix Sys., Inc.*, 889 F.3d 735, 742-

743 (Fed. Cir. 2018). Indeed, that is likely why Centripetal's defense of the claims' validity

before the PTAB did not frame the "particular type of data transfer" to include all packets from

quarantined computers in the first network, but instead framed it more narrowly. DTX-369

at .010 ("types of data transfers associated with communications protocols other than HTTP and

HTTPS"); *id.* at .017 ("'**the second stage** may determine if the policy allows the specific method

or type of communication (e.g. file read, file write, encrypted communication, etc.) between the

resources'" (emphasis Centripetal's) (quoting '193 patent at 8:48-51)); *id.* at .021 ("**a particular**

method associated with a data transfer protocol" (emphasis Centripetal's) (quoting '193 patent at

2:24-29)); Tr. 2426:5-21 (Crovella); Op. 26.

C.   Centripetal Shows No Basis For Reopening The Record

Centripetal next demands that the Court reopen the record to allow it to show

infringement "under the new construction the Court adopted." Mem. 9. But the Court did not

adopt any "new construction," so there is no basis for reopening the record to address a

nonexistent issue (or assert a new infringement theory). Rather, the Court simply applied the

claims' dispositive requirement that "one or more packet-filtering rules" filter packets in two

stages (according to source/destination and particular type of data transfer criteria). This was no

surprise to Centripetal, and Centripetal's motion does not argue otherwise. Not only does the

Court's decision track the two-stage filtering method that the patent itself discloses and claims—

and that Centripetal itself advocated before the PTAB—but Cisco has consistently explained that

approach throughout the case, from the 2020 trial through the Rule 63 proceeding.[4] The Court

itself asked Centripetal's counsel about it. Rule 63 Tr. 248:16-24. Accordingly, Centripetal had

every opportunity to respond to Cisco's contentions.

Nor is there any basis to allow Centripetal to introduce new evidence and recall witnesses

to present its "segmentation" and "microsegmentation" arguments in support of a newly

fashioned infringement theory. Mem. 10-12. Centripetal does not suggest that such evidence,

including the material proffered with its motion, was unavailable during the trial or Rule 63

hearing. Indeed, Centripetal presented those arguments through cross-examination of Cisco's

tutorialist Dr. Almeroth (Rule 63 Tr. 164:5-168:17), closing argument (Rule 63 Tr. 251:4-8,

---

[4] *See, e.g.*, Tr. 2355:4-22, 2362:9-2363:3, 2370:12-2372:25, 2375:2-2377:1, 2387:2-13, 2404:23-
24; 2405:8-16; 2423:25-2424:15; 2425:17-2426:21 (Crovella), 3274:10-3280:20 (Cisco's
closing); Rule 63 Tr. 297:8-25, 301:1-304:21, 314:8-14 (Cisco's Rule 63 closing); *see also* Dkt.
167 at 17-18; Dkt. 445 at 24 (explaining that Cisco's quarantine rule cannot infringe because "it
cannot identify *any particular* types of data transfer," but is "instead a tool that a human being
can use to block all traffic to certain destinations" (emphasis original)); Dkt. 474 at 23-24(¶¶82-
85); Dkt. 698 at 9-13; Dkt. 737-1 at 15(¶37), 19-27(¶¶46-49, 50-64).

265:21-268:10), and reading from, and offering as evidence, some of the very language belatedly discussed in Dr. Mitzenmacher's declaration.[5]

Moreover, Centripetal's new argument would, once again, require redoing the case completely. That is because the only "packet-filtering rules" that Centripetal accused at the original trial were "quarantine" rules,[6] not some combination of "quarantine" rules and other rules, as the Court itself noted. Op. 29 n.10. Now, however, Centripetal ventures a vague argument based on ***different, unspecified rules***, namely "***the rules*** that the Switches and Routers employ [that] ***may*** operate only on packets with a certain traffic type or ***payload information***." Mem. 10. Centripetal does not explain what "rules" it is talking about—they are certainly not quarantine rules, which do not operate on "payload information," but on source and destination. Tr. 2400:11-25, 2403:22-2404:5 (Crovella); Tr. 869:1-12 (Mitzenmacher); Dkt. 478-1 at 3(¶13). Centripetal's prior focus on quarantine rules is understandable given Centripetal's mapping of ***other*** claim elements, which required that the accused rules originate from ISE as a result of a Stealthwatch alert; Centripetal has not explained how any non-quarantine rule could satisfy those elements. Dkt. 737-1 at 12, 28, 40, 193-195(¶¶30, 67, 89, 464, 466); Dkt. 725 at 35-36, 46(¶¶153-154, 159-160, 207 (*e.g.*, relying on CTA documents and code (PTX-1911, PTX-576, PTX-1849 at 228))); Rule 63 Tr. 298:7-15. Centripetal proffered no expert testimony mapping non-quarantine rules against the other claim elements; Cisco has not been able to cross-examine any witnesses or present rebuttal evidence on such a theory; and Cisco would need the opportunity to develop a corresponding invalidity case that its prior art products employed the

---

[5] *Compare, e.g.*, Rule 63 Tr. 165:3-9 *with* Dkt. 790(¶5) (quoting same language from Dkt. 790-1 at 1); *compare also* Rule 63 Tr. 166:16-19 *with* Dkt. 790 at 3(¶6) (quoting same language from Dkt. 790-1 at 2); *see also* Rule 63 Tr. 165:14-166:14; Rule 63 Tr. 188:16-19.

[6] *See, e.g.*, Tr. 791:14-792:24, 2377:13-2379:1; Dkt. 475(¶¶9-10); Dkt. 725 at 35-36; Rule 63 Tr. 305:4-306:16.

same accused rules as Centripetal's revised infringement theory. *See 01 Communique*, 889 F.3d at 742-743. This is all the more reason to reject Centripetal's new argument, particularly given its refusal to recall witnesses in the Rule 63 proceeding, notwithstanding its full awareness of Cisco's noninfringement positions.[7]

> **D.   Centripetal Shows No Error In The Court's Factual Findings Regarding The Accused Products' Functioning**

Centripetal additionally accuses the Court of misunderstanding how the accused quarantine rules work (Mem. 11-13), but Centripetal's own expert admitted that quarantine rules "restrict according to source and destination." Tr. 528:3-4; *see supra* p. 4. Centripetal now asserts that that "the Switches and Routers cannot effectuate a quarantine by performing a simple source and destination check," but cites no evidence supporting that proposition. Mem. 13. While its motion cites certain trial testimony (Mem. 12 (citing Tr. 468:8-17, 489:22-490:16, 535:21-24)), it provides no quotations or explanatory parentheticals. Not surprisingly, the passages only confirm that Cisco's quarantine rules block packets based on source and destination.[8] Centripetal's cited exhibits likewise add nothing. One of them even confirms that security group access control lists (SGACLs)—of which the only accused rule (the quarantine

---

[7] *See, e.g.*, Dkt. 656 at 1-2 ("Centripetal proposes that the Court … should … decide this case based on the current record"; arguing that recalling witnesses "will be unnecessary and wasteful"); Dkt. 663 at 5:14-16 ("There's been a tremendous record below, and we don't want to just start over again and redo that. I think that would be a tremendous waste of resources."), 6:5-12, 7:10-14, 28:1-29:2, 30:11-17; Dkt. 675 (Transcript of 1-25-2023 Status Hearing) at 17:8-18:3, 22:12-23:24, 25:2-11.

[8] Tr. 468:8-17 ("So what this slide is showing … is that you can have packets that ***there's places from your internal network that it may be okay to reach***, either okay to send or to get information from, and there may be applications that it's not okay to reach, and in that case, you know, packets should be denied."), 489:22-490:16 ("I might have a rule put in place that says, look, ***I'm not going to allow this user to access certain locations***, you know."), 535:21-24 ("[I]t might be the same that ***you can only go to these other groups***, or in particular it might also be ***you can only go to these networks or parts of the network***.").

11

SGACL) is one type—"limit the endpoint's network access"—*i.e.*, they restrict according to

source ("endpoint") and destination ("network access"). PTX-1280 at 21. Centripetal's expert

confirmed as much. Tr. 496:12-498:14, 498:23-499:8; Rule 63 Tr. 306:1-25.[9]

Finally, Centripetal's demand for "an amended judgment of infringement" (Mem. 8) is a

non-starter no matter what. Any one of Cisco's additional noninfringement and invalidity

contentions—which the Court did not address—would separately warrant judgment for Cisco.

Op. 20 n.7, 61 n.21; Dkt. 737-1 at 10-13(¶¶25-32), 50-54(¶¶107-113).

II.   The '806 Patent

A.   The Court Properly Rejected Centripetal's Infringement Theory

Even though Centripetal had hundreds of pages and hours of argument to explain its

infringement theory for the '806 patent, it now argues that the Court completely misunderstood

it. On the contrary, the Court understood it perfectly and properly rejected it based on the

evidence. None of Centripetal's scattershot arguments shows otherwise.

First, Centripetal alleges that the Court "did not address" Centripetal's assertion that the

Cisco accused products supposedly "stop processing packets with the old rule set and cache

those packets *while it completes the rule swap*." Mem. 15 (emphasis Centripetal's); *see also*

Mem. 18. Centripetal is plainly wrong. The Court repeatedly acknowledged Centripetal's focus

on the products' operation ***during a rule swap***. *E.g.*, Op. 38 ("At various points, [Dr.

Mitzenmacher] described the ceasing and caching of packets as occurring *during* a rule swap,

rather than because of it." (emphasis the Court's)), 39 ("Dr. Mitzenmacher explained that the

---

[9] Centripetal's other cited exhibits merely illustrate the order in which various unaccused rules are applied, which in no way undermines its expert's admission that implementing the accused quarantine rules filters by source and destination. PTX-1390 at 86 (illustrating the "Order and Priority" of various unaccused rules); PTX-1276 at 216 (similar); PTX-1193 at 007 (prior art).

inclusion of this feature indicated to him that the accused devices would need to cease processing

packets *during a rule swap*."), 41 ("Centripetal argued … that the Accused Switches cease

processing responsive to a signal to swap to a new rule set.").

Centripetal does not like the Court's comparison of what happens during a rule swap to

what happens in "normal packet processing" (Mem. 15), but the claims themselves make that

relevant. The "cease processing" and "cache" requirements do not exist in a vacuum; the

processor must perform these actions "***responsive to being signaled*** to process packets in

accordance with the second rule set." '806 patent at 11:39-44, 12:51-55. *See IGT v. Bally*

Gaming Int'l Inc., 610 F. Supp. 2d 288, 332 (D. Del. 2009) ("'responsive to'" means "in reply or

reaction to [an] occurrence"), *aff'd*, 659 F.3d 1109 (Fed. Cir. 2011); *Intel Corp. v. Broadcom*

Corp., No. Civ.A. 00-796-SLR, 2003 WL 360256, at *7-8 (D. Del. Feb. 13, 2003) (defining

"responsive" in claim limitations reciting "responsive to a control signal" as "to respond or

react"). The most logical way to determine whether this explicit causation requirement is

satisfied is to compare packet processing during normal operation (when there is no "signal[] to

process packets in accordance with the second rule set") with packet processing during the rule

swap (when, on Centripetal's theory, there would be such a signal). If there are no changes to

packet processing during the rule swap (as is true for Cisco's accused products), then packet

processing is not "cease[d]" and packets are not "cache[d]" "***responsive to being signaled*** to

process packets in accordance with the second rule set." The Court correctly explained this point

at length, Op. 37-41, including noting that Dr. Mitzenmacher did not address the causation

requirement, Op. 38.

Second, Centripetal contends that "the rule swap will ***change the normal processing of***

packets" and "cause[] ***different actions*** to take place than what otherwise would have occurred

13

during normal packet processing." Mem. 15-16. This is a new argument on which Centripetal

proposed no findings, and can be rejected on that basis. *See* Dkt. 475 at 10-13 (¶¶47-75); Dkt.

725 at 60-61 (¶¶277-279); Dkt. 702 at 11-13. Centripetal does not say what "change[s]" and

"differen[ces]" it has in mind, but the patent claims are specific: the signal to swap rule sets must

cause ("responsive to being signaled") packet processing to "cease" and packets to be

"cache[d]." '806 patent at 11:39-44, 12:51-55. The evidence is overwhelming that Cisco's

products do not do this, Op. 37-44, and Centripetal has no response.[10] To the extent that

Centripetal is arguing that the rule-swap process alters the timing of when packets are processed,

e.g. Mem. 16 ("Since there are no rules to be applied while rules are being swapped, there is no

processing of any packets during this time[.]"), the Court rejected this argument based on

overwhelming evidence, Op. 38-42. As the Court found, the only change that occurs as a result

of a rule swap is that one packet is processed according to the old rule set, and then the next

packet is processed according to the new rule set—a seamless process that does not affect the

timing of packet processing. Op. 41-42. Centripetal has no basis to question these findings.

  Third, Centripetal now claims that Cisco's "rule-swapping process … interrupts normal

packet processing," Mem. 16, which supposedly "meets the 'cease processing' of packets

element," Mem. 18. This is yet another new argument on which Centripetal proposed no

findings. *See* Dkt. 475 at 10-13(¶¶47-75); Dkt. 725 at 60-61(¶¶277-279); Dkt. 702 at 11-13.

The material Centripetal cites (Mem. 16-17) does not support its assertion, and indeed shows just

---

[10] Centripetal argues, citing Dr. Mitzenmacher's testimony, that "[t]he Firewalls also cannot process packets during rule swapping, because the memory is being used to change the rule sets." Mem. 16 (citing Tr. 704:23-705:10). Again, this is irrelevant even if believed, because the rule set is swapped during the time between the firewall's normal processing of individual packets; the firewall does not "cease" processing packets "responsive to being signaled" to change rule sets. Op. 36; Tr. 2521:6-12, 2522:8-15.

the opposite. For example, PTX-1303, a Cisco document cited by the Court (Op. 20, 33) and Centripetal's expert (Tr. 477:2-478:14, 629:23-630:19), states that the accused "Hitless TCAM Update" "[a]llows updates to an ACL *without interrupting traffic*." PTX-1303 at 73; *see also* Tr. 2550:12-2552:25 (Cisco's Peter Jones testifying that accused Catalyst switches use Hitless ACL update). Dr. Mitzenmacher confirmed the same. Tr. 630:5-19 ("So it's saying that this is a feature they're bringing out that will, you know, improve performance by allowing updates, *without interrupting the traffic*.").

Fourth, Centripetal argues that, unlike Cisco's "old system" that would "drop" packets during a rule swap due to conflicts between the old and new rule sets, the accused products only use one rule set at a time. Mem. 14, 17-18. The Court acknowledged this argument, but found it immaterial because "this does not mean that the ceasing and caching operations are done 'responsive to' the rule swap." Op. 39-40. Centripetal does not mention this part of the Court's Opinion, much less refute it. Centripetal's repeated references to differences between Cisco's "old system"/"old regime" and the accused products (Mem. 14, 17, 21) are also irrelevant, as Centripetal's burden is to compare the accused products to *the claims*, which include the "cease processing" and "cache" requirements that the accused products do not practice.

Fifth, Centripetal argues that "the signal to switch rule sets causes the accused network devices to cache packets" by supposedly causing the accused products to switch from the "default setting" of "drop[ping] packets" to caching them. Mem. 18. This is yet another new argument, which is why Centripetal is unable to cite any *testimony* explaining what the source code it cites (PTX-1849 at 21, 29) actually does. *See, e.g.*, Dkt. 475 at 10-13(¶¶47-75), Dkt. 725 at 60-61(¶¶277-279) (Centripetal findings of fact/conclusions of law not citing PTX-1849 for "cease processing" or "cache" requirements). Centripetal's attorney argument cannot fill that

15

gap. In any event, Centripetal's unsupported assertion is wrong. PTX-1303, on which Dr.

Mitzenmacher relied (Tr. 629:23-630:19), states that "***Hitless update is enabled by default***; can't

be disabled." PTX-1303 at 73. In other words, the default is not "to drop packets," but to

continue to process packets with the old rule set until the new rule set is ready. Tr. 2552:18-25,

2554:12-24. Moreover, the signal to switch rule sets does not "cause[]" the accused products to

cache packets, as Centripetal alleges, Mem. 18; instead, as the Court correctly found, the accused

products buffer packets (the alleged caching) in the same way whether or not a rule swap occurs,

Op. 34(¶29), 36-37(¶36), 38-41; Dkt. 737-1 at 76-78(¶¶159, 161-162).

>   **B.**   **The Court Did Not Misconstrue "Cease Processing"**

Centripetal next contends that the Court should have construed "cease processing of one

or more packets" not to mean what it says, but instead as though it read "stop processing with the

old rule set," Mem. 19 (citing Op. 41-44). Centripetal has never articulated any developed claim

construction argument justifying that reading, and that is no surprise: as the Court correctly

noted, Op. 42, Centripetal's interpretation impermissibly adds language to the claims, which

recite "cease processing of one or more packets," not "cease processing of one or more packets

with the old rule set." '806 patent at 11:43, 12:54. Centripetal does not even attempt to

reconcile its position with the actual claim language, instead jumping straight to the

specification. Mem. 19. But the specification cannot be used to contradict the claim language.

See Buckingham Mfg. Co. v. Bashlin Indus., Inc., 2022 WL 17668809, at *14 (W.D. Pa. July 8,

2022) (rejecting construction that "adds words to the claims that are not present"); *Leviton Mfg.

Co. v. Universal Sec. Instruments, Inc.*, 304 F. Supp. 2d 726, 739 (D. Md. 2004) (similar).

In any event, Centripetal's specification-based arguments fail. Centripetal seizes on the

statement that "upon ceasing to process packets (e.g., when a current packet has been examined

against the rules in policy 130's rule set), each of processors 300, 302, and 304 may signal

administrative processor 312 that they have stopped processing packets." '806 patent at 8:4-8 (cited at Mem. 19). But this is merely an acknowledgement that a system that processed packets with a first rule set, and then "stopped processing packets" altogether—full stop—also necessarily stopped processing packets with the first rule set. That does not remotely suggest that "cease processing one or more packets" ***should be redefined as*** "cease processing one or more packets ***with the old rule set***," as Centripetal argues. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) ("we look to the words of the claims themselves … to define the scope of the patented invention" (quotation marks omitted)); *Buckingham*, 2022 WL 17668809, at *14; *Leviton*, 304 F. Supp. 2d at 739. Indeed, Centripetal's overbroad interpretation would produce absurd results. A system that "cease[s] processing one or more packets with the old rule set" could continue processing packets with no rule set at all, allowing packets to pass through the system unexamined, which is contrary to the '806 patent's stated purpose of mitigating the effects of an attack. *See* '806 patent at 8:37-53; Tr. 620:4-6 (Mitzenmacher: "You don't want to accidentally let a packet through that shouldn't get through because you're in a state of flux."). Neither the patent nor any Centripetal witness suggested that it would be desirable to allow some packets to be processed without applying any rule set at all.

Centripetal argues that "there is no evidence in the record of any disclaimer" (Mem. 19)—a curious assertion, given that the Court did not rely on disclaimer and had no reason to. Disclaimer narrows a claim's ordinary meaning based on statements in the specification or prosecution history. *See Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003). Here, it is ***Centripetal*** who seeks to alter the claim language by contorting statements in the specification, thus violating the "heavy presumption that claim terms carry their full ordinary and customary meaning." *Id.* at 1323 (quotation marks omitted).

17

Centripetal further alleges that the Court treated Figure 4 "as a limitation on the claims," Mem. 19, but the Court did no such thing. The Court (Op. 42-43) cited Figure 4 as *confirming* the claims' plain meaning, which it clearly does by describing step 404 as "PROCESSORS CEASE PROCESSING PACKETS." Centripetal points to language stating that processors "may cease processing packets in accordance with policy 300's rule set," '806 patent at 9:4-8 (quoted at Mem. 20), but again, that simply reflects the fact that a system that ceases processing packets altogether necessarily ceases processing packets with the first rule set. It is not a basis to redefine the unambiguous claim language to allow processing to continue unceased, potentially even without applying any rule set.

Moreover, the specification abounds with statements confirming the claims' plain language and contradicting Centripetal's rewriting. *See, e.g.*, '806 patent at 1:62-64 ("the processors may *cease processing packets* and may cache any unprocessed packets"), 7:57-63 ("In some embodiments, each of processors 300, 302, and 304 may finish processing the packet they are currently processing and then *cease processing packets*. In other embodiments, each of processors 300, 302, and 304 may *cease processing packets* and cache the packet they are currently processing for future processing in accordance with policy 132's rule set."), 7:38-41 ("[E]ach of processors 300, 302, and 304 may be *signaled* by administrative processor 312 (e.g., via data bus 120) *to stop processing packets*."), 8:6-10 (similar). And as the Court highlighted and Centripetal's motion does not address, Centripetal's own expert described the claim requirement as "to stop processing *any packets*." Op. 43 (citing Tr. 620:1-4); *see also* Tr. 619:15-620:16 ("So once you're starting to do the swap for the second rule set, you want to stop processing any packets. … So what you have to do is *stop processing for anything coming in*, and anything that you would normally process, you're going to cache.").

Centripetal also baselessly asserts that it lacked "notice of the Court's interpretation of this claim limitation." Mem. 20. But Centripetal has known *for years* that Cisco's noninfringement positions relied on the plain meaning of the "cease processing" and "cache" limitations. *E.g.*, Dkt. 474 at 32-35(¶¶114-123); Tr. 3293:12-3299:24; *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, No. 2021-1888 (Fed. Cir.), Dkt. 18 at 23-28 (Cisco's Federal Circuit brief). And this contention was reiterated countless times during the Rule 63 proceeding, including in questions from the Court. *See, e.g.*, Rule 63 Tr. 372:10-373:21, 381:22-391:24, 394:22-402:6; *id.*, 353:12-22, 369:1-23, 413:23-414:17 (Centripetal's closing, including Court questions regarding claim interpretation); Dkt. 698 at 24-29; Dkt. 737-1 at 85-98(¶¶182-209). The Court's plain-meaning interpretation was also the one Dr. Mitzenmacher used. Tr. 619:15-620:16. Centripetal thus had every reason to anticipate that the Court could interpret the claims the way it did, and it was obligated to present all of its evidence and arguments accordingly. *See, e.g.*, *Intellectual Ventures II LLC v. Ericsson Inc.*, 686 F. App'x 900, 905 (Fed. Cir. 2017).

Even if Centripetal's "cease processing" interpretation were correct (it is not), judgment of noninfringement would still be warranted. Centripetal's "cease processing" claim construction argument does not affect the Court's finding that Cisco's accused products do not "cache the one or more packets" "responsive to being signaled," Op. 37, 40—an independent basis supporting the noninfringement judgment.

C.   The Court Did Not Import A Limitation Into The Claims

Finally, Centripetal accuses the Court of "comparing Cisco's accused products to the specification," Mem. 20, based on the Court's observation that "the problem that the ['806] patent was designed to solve—processing packets with an outdated rule set—*still occurs in the accused devices*," Op. 44 (emphasis the Court's). But the Court did not find noninfringement "*because* [Cisco's accused products] continue to process packets with an outdated rule set while

19

configuring a new rule set," Mem. 20 (quotation marks and brackets omitted); the Court stated

only that this fact "***further supported***" (Op. 40) the noninfringement finding the Court had

already reached due to Centripetal's failure to show infringement, Op. 37-43. It is not error to

note that the Court's understanding of the claims is consistent with the specification. Moreover,

any error—though there is none—would be harmless; even if the two paragraphs discussing the

"problem" addressed by the '806 patent (Op. 44) were removed from the Opinion, the substance

of the Court's analysis would not change.

Centripetal wrongly attempts to discount Mr. Shankar's testimony as "describ[ing] what

occurs during normal packet processing *before* any signal to swap rules has been sent." Mem. 21

(emphasis Centripetal's). Mr. Shankar was addressing the question "why it's ok … to use the

old rule set ***while the new rule set is being programmed***," Tr. 2518:22-2519:7—the very tactic

the patent criticizes. '806 patent at 1:25-31 ("***while implementing a new rule set*** … processing

packets in accordance with an outdated rule set … may exacerbate rather than mitigate the

impetus for the rule set switch"); Op. 44 (citing Tr. 2518:22-2519:7, PTX-1196 at 007).[11]

III.   The '176 Patent

A.   The Court Correctly Determined That Cisco's Accused Products Do Not Practice The Claimed "Correlation" Requirement

1.   Centripetal Presented No Credible Evidence That Cisco's Products Compare Ingress And Egress NetFlow Records

For the '176 Patent, Centripetal first argues that the Court erred in finding that Cisco's

accused products do not compare ingress NetFlow records for a device with egress NetFlow

---

[11] Centripetal's request for "an amended judgment of infringement" of the '806 patent (Mem. 22) is again unwarranted, because the Court did not address Cisco's additional noninfringement and invalidity contentions. Op. 35 n.12, 38 n.15, 61 n.21; Dkt. 737-1 at 10-13(¶¶25-32), 98-100(¶¶210-212), 101-105(¶¶216-227); *supra* p. 12.

records from that device to correlate received and transmitted packets for that device. Mem. 23-25. But the Court correctly found that Centripetal failed to prove the claimed correlation, and the Cisco evidence Centripetal complains about merely confirmed this deficiency.

Centripetal begins by recounting Dr. Cole's testimony on the correlation requirement and related documents, but fails to show how the Court supposedly misevaluated this evidence. Mem. 23. The Court meticulously explained how Centripetal failed to carry its burden of proving the claimed correlation. Op. 54-58. The Court noted that Dr. Cole offered no testimony regarding source code or testing for the correlation element, but instead relied on three Cisco documents, each of which the Court examined and found (as Cisco had argued[12]) that none reflects the claimed correlation. Op. 56-58. The Court then found that Dr. Cole's testimony on the correlation requirement deserved "little weight" as it was conclusory and not supported by the evidence he cited. Op. 58. Centripetal entirely ignores this portion of the Court's Opinion. *Compare* Op. 54-58, *with* Mem. 22-28.

Only *after* the Court established Centripetal's failure of proof on the correlation requirement did it turn to *Cisco's* additional evidence, which the Court found further "bolstered" its noninfringement finding. Op. 58-59. Centripetal's motion focuses on the Court's discussion of Cisco's evidence, Mem. 23-25, but never grapples with the Court's threshold finding that **Centripetal's own proffered evidence** did not carry Centripetal's burden of proving the claimed correlation. *See* Op. 53-54 ("Centripetal has failed to show that the accused technology correlates the packets entering and exiting a network device." (internal numbering omitted)). This failure alone warrants denying Centripetal's motion.

---

[12] *See* Dkt. 737-1 at 119-147(¶¶259-321); Rule 63 Tr. 526:11-532:5, 537:15-538:10.

Nonetheless, the Court correctly found that Cisco's additional evidence confirmed that its accused products do not perform the claimed correlation. Op. 58-59. The Court discussed evidence that egress NetFlow records are not compared to ingress NetFlow records to perform the claimed correlation because (1) Cisco's technical documents show that enabling routers and switches to export both ingress and egress NetFlow records could result in double counting if both are exported;[13] (2) if a customer enables exporting both ingress and egress NetFlow, source code instructs the Stealthwatch Flow Collector to "ignore egress"; (3) Cisco engineer Danny Llewallyn testified that Stealthwatch was built to assume that all ingested NetFlow records are ingress records; and (4) Mr. Llewallyn testified that even if (in a hypothetical scenario) both ingress and egress NetFlow records were exported to Stealthwatch, the distinction between the two would be lost before they are ingested by Stealthwatch, meaning that the alleged correlation would be impossible. Op. 58-59. Centripetal argues that these findings do not ***foreclose*** the accused products from performing the claimed correlation. *See* Mem. 23-24. But that is beside the point since, as the Court found and Centripetal does not refute, Centripetal failed to show that the Cisco accused products are even capable of performing, let alone perform, the claimed correlation in the first place. Op. 54-58.

Moreover, as the Court noted, Cisco's additional evidence "bolster[s]" the Court's finding that Centripetal failed to prove the claimed correlation. Op. 58. If Stealthwatch actually relied on egress NetFlow records to perform correlation, then Cisco would not have instructed

---

[13] Centripetal claims that Dr. Almeroth "erroneously calls this miscounting an 'error condition,'" and that "Mr. Llewallyn did not use this term." Mem. 24 n.5. Centripetal is wrong; Mr. Llewallyn used this very language. Tr. 2182:21-25 ("A. No, [ingress and egress NetFlow records are] really duplicates. You get duplicate records, which causes a doubling of the statistics. So that's why Stealthwatch can do everything it does with either side. They're just duplicate records. One has to go; otherwise, it's an ***error condition***.").

customers to avoid exporting egress NetFlow to Stealthwatch, and would not have provided

source code instructing the Stealthwatch Flow Collector to "ignore egress." That Cisco has

taken affirmative steps to prevent Stealthwatch from receiving or recognizing egress NetFlow

records further confirms that Stealthwatch does not use egress records to perform the claimed

correlation (much less generate rules in response).

2. Centripetal's Only Infringement Theory Was Based On NetFlow

Centripetal also argues that the Court erred by not considering supposed correlation when

the accused products (1) deduplicate NetFlow records and (2) use proxy data in the form of

Syslog or WebFlow. Mem. 25-27. Both assertions are meritless.

a. Deduplication

Centripetal's argument regarding deduplication of NetFlow records fails for several

reasons. *First*, Centripetal did not present this theory at trial. Dr. Cole did not mention

deduplication *once*. *See generally* Tr. 873-1142. And Centripetal did not mention deduplication

in *any iteration* of its proposed findings of fact and conclusions of law. *See generally* Dkt. 419,

475, 725. The Court was not required to consider a theory Centripetal did not raise. *See supra*

pp. 7-8 (citing cases). Indeed, to rely on it would have unfairly prejudiced Cisco, as Cisco would

not have been able to cross-examine any Centripetal witnesses or adduce its own expert

testimony on it, as to both noninfringement and invalidity.

Second, and confirming why the adjudication of this new theory would have required the

reopening of discovery and recalling of witnesses on both sides, the deduplication theory

Centripetal now asserts is inconsistent with the infringement theory Centripetal did present at

trial. As Dr. Cole testified, Centripetal's trial theory was that the alleged correlation was

performed by Cognitive Threat Analytics (CTA). Tr. 1107:23-1108:10; Rule 63 Tr. 477:13-

478:3, 511:18-512:18. But NetFlow deduplication is performed by the Stealthwatch Flow

23

Collector, not CTA. *See* Tr. 2147:7-22 (Mr. Llewallyn describing that the Stealthwatch Flow

Collector receives the NetFlow records, builds the "StealthWatch flow," and sends that to CTA),

2181:12-2182:15 (explaining that Flow Collector discards NetFlow records and there is no

concept of ingress or egress in the Stealthwatch flow sent to CTA).

 Third, NetFlow deduplication could not have been a viable infringement theory in any

event, because no rule is generated "in response to" deduplication, '176 patent at 17:26-31,

19:14-19—instead, deduplication is "about eliminating duplicates," Rule 63 Tr. 177:25. Had this

been Centripetal's infringement theory, Cisco would have called fact and expert witnesses to

prove that the duplicative information is discarded. Dkt. 626-1, Exhibit A(¶¶4-8). Even

Centripetal admitted that NetFlow deduplication does not satisfy the claim requirement of

"responsive to correlating … generate, based on the correlating, one or more rules." *See* Dkt.

629 at 11 (statements about "de-duplication of Netflow records" "are irrelevant to generating

rules responsive to correlation, which the claims require").

 Finally, Centripetal alleges that Dr. Almeroth stated (on cross-examination during his

tutorial) that "during deduplication, ingress and egress flows are compared and deduplicated."

Mem. 25. But Dr. Almeroth's cited testimony (Rule 63 Tr. 177:14-178:1) says nothing about

comparing ingress and egress NetFlow records (or any other kind of logs) for a network device.

Indeed, he stated just the opposite—that deduplication is "not about correlating ingress with

egress." *Id.* at 177:22-178:1. And the notion that Centripetal, having declined to recall any

witnesses, can present a new infringement theory based on the cross-examination of Cisco's

tutorialist strains credulity. Centripetal also suggests that Mr. Llewallyn testified that NetFlow

records are correlated. Mem. 25 n.6. Again, the cited testimony is different: Mr. Llewallyn

merely agreed that the Stealthwatch Flow Collector can receive NetFlow records from multiple

switches and routers between two computers, not that it compares ingress and egress NetFlow records to correlate packets received with packets transmitted for a particular network device. Tr. 2149:13-18. Indeed, deduplication only takes place for NetFlow from *different* network devices, not ingress and egress NetFlow from the *same* network device (Rule 63 Tr. 177:19-178:1), as the claims would require (Op. 49 n.16, 59 n.20).

b.   Proxy data

Centripetal further argues that the Court erred by not considering whether Stealthwatch performs the claimed correlation based on proxy data in the form of WebFlow or Syslog. Mem. 26-27. That argument, too, is unavailing.

First, as the Court explained (Op. 55), Dr. Cole's infringement theory relied on correlation involving NetFlow records, not proxy data. His direct testimony mentioned Syslog a single time (Tr. 985:6) and WebFlow twice (Tr. 996:24, 999:1), but in none of these instances did he assert that (much less explain how) Cisco's accused products compare ingress Syslog/WebFlow/NetFlow to egress Syslog/WebFlow/NetFlow to correlate received and transmitted packets. Centripetal confirmed its lack of reliance on proxy data for infringement:

> THE COURT: I mean, because I want to be clear that I understand what you're alleging infringes, and *I don't think you've alleged here that it's the proxy data*.

> MR. ANDRE: I think the evidence shows that *the NetFlow data is what we're accusing of infringing*.

Rule 63 Tr. 482:21-25. Nor was this exchange "only about the use of NetFlow records," Mem. 27; the Court explicitly asked whether Centripetal accused "proxy data." *Id.* at 482:21-23.

Second, even putting this waiver aside, Centripetal did not offer *any* evidence showing that the Cisco accused products "generate a plurality of log entries" in the form of Syslog/WebFlow proxy data—instead relying entirely on NetFlow for these limitations. Tr.

25

977:13-993:18, 1104:2-15. This lack of evidence is fatal to any argument that Syslog/WebFlow

data meet the correlation requirement, because the log entries that are "generate[d]" are the ones

that must later be used for "correlat[ing]" packets ("correlate, based on *the* plurality of log

entries"). *See* Op. 49 n.16, 59 n.20 (discussing antecedent basis requirement). Having offered

no evidence that the Cisco accused products "generate" Syslog/WebFlow, Centripetal cannot

prove infringement by arguing that Syslog/WebFlow are used for correlation.

 Third, proxy data is generated by non-accused ***proxy servers***. *See* Op. 56; PTX-1065 at

005 (figure from Cisco document relied on by Dr. Cole showing "Proxy Data" generated by a

"Web Proxy," not a Cisco accused product); Dkt. 725 at 75, 85(¶¶351, 382) (Centripetal

admitting Stealthwatch receives Syslog "from proxy sources" and WebFlow is "produced by

Syslogs"); Dkt. 626-1, Exhibit A(¶¶9-11) (Mr. Llewallyn confirming that proxy data is generated

by unaccused proxy servers). As the Court noted (Op. 55), Dr. Cole confirmed that proxy

servers are not at issue. Tr. 978:14-18 ("[W]ith the '176 patent, there's actually not a proxy in

the claim language. So we don't actually have a proxy in this case. We just have to show that

the router or switch receives packets and logs and transmits packets and logs.").

 Finally, even putting aside these numerous flaws, Dr. Cole's testimony about

Syslog/WebFlow was even more vague than the testimony about NetFlow that the Court found

deficient. Op. 58; Tr. 985:6, 996:24, 999:1. Centripetal's only attempt to explain its

Syslog/WebFlow theory is to argue that "data from NetFlow and WebFlow are for different

packets, and any argument about ignoring egress packets is irrelevant because there is no double

counting of packets." Mem. 26. But even if that were true, Centripetal again offered no specific

evidence that the Cisco accused products compare ingress Syslog/WebFlow/NetFlow to egress

Syslog/WebFlow/NetFlow to perform the claimed correlation. *Cf.* Op. 54-58. In other words,

even were the Court to consider Syslog/WebFlow, Centripetal failed to prove infringement for the same reasons the Court has already identified regarding NetFlow.

3.   The Court Did Not Import Limitations Into The Claims

Centripetal raises another last-ditch argument that the Court somehow reconstrued the claims, asserting that the Court imported a "packet obfuscation" requirement from the specification into the claims. Mem. 27-28. Once again, the Court did no such thing.

The Court explained in detail how Centripetal failed to prove that Cisco's products satisfied the plain meaning of the correlation requirement. Op. 53-59. Only ***afterwards*** did the Court add that its conclusion is "***further supported*** by considering the problem that the '176 Patent was designed to solve—packet obfuscation by a network device." Op. 59. That is not importing a "packet obfuscation" requirement from the specification, nor is it even claim construction. It is simply noting that the Court's conclusion is consistent with the specification, because Cisco's accused products "do not have the problem that the '176 Patent was designed to solve." Op. 59. Again, if this entire paragraph were removed from the Court's Opinion, the Court's analysis would not change at all.

Because the Court did not import a "packet obfuscation" requirement, there is no basis for Centripetal's belated "Network Address Translation" ("NAT") infringement theory, raised for the first time in Dr. Cole's post-judgment declaration. Mem. 28; Dkt. 792. Dr. Cole admits that he "did not testify about" this NAT theory at trial, Dkt. 792(¶6), and it is not mentioned in any iteration of Centripetal's proposed findings of fact and conclusions of law, Dkt. 419, 475, 725.[14] NAT was also long known in the prior art, and again would have been a basis for a new

---

[14] Although Centripetal did not present an infringement theory based on Network Address Translation, it did briefly cross-examine Dr. Almeroth on this topic at trial, and he testified that NAT "is ***not correlation*** as described by the claims." Tr. 2297:5-2298:16.

invalidity theory. There is simply no basis to reopen the record to allow Centripetal to present an

entirely new infringement theory in response to a (once again) nonexistent claim construction.

> **B.   The Court Correctly Determined That Cisco's Accused Products Do Not Generate Or Provision Rules In Response To Correlation**

Lastly, Centripetal argues that the Court erred in separately determining that Stealthwatch

does not "generate[], based on the correlating, one or more rules configured to identify packets

received from the host located in the first network" or "provision[] a device" with those rules.

Mem. 28. None of Centripetal's arguments has merit.

Dr. Cole admitted that the supposed "rule" generated by the Cisco accused products is an

"alert or alarm" "generate[d]" by Stealthwatch in conjunction with CTA and "provision[ed]" to

the Stealthwatch Management Console. Tr. 1112:23-1114:6. As the Court explained, these

alerts do not satisfy the agreed claim construction of "rule" as "a condition or set of conditions

that when satisfied cause a specific function to occur." Op. 60 (citing *Markman* Order at 9).

That is because when CTA sends an alert to Stealthwatch, the alert does not "cause a specific

function to occur," but instead merely alerts a human administrator to suspicious activity that

may warrant remedial action. Tr. 2265:2-2268:15, 2261:9-2263:10, 2183:25-2191:14; Rule 63

Tr. 522:6-532:2. Centripetal's motion does not even mention these CTA alerts that formed the

basis for Dr. Cole's infringement opinion, much less explain how the Court supposedly erred in

finding that they are not "rules." No more is needed to deny Centripetal's motion as to the

"generate … one or more rules" requirement.

Moreover, despite admitting that his infringement theory was limited to CTA alerts, Dr.

Cole relied upon PTX-1089 at 1238 to vaguely suggest that a quarantine command to ISE could

be the claimed "rule." Tr. 1002:4-1003:1. But as the Court explained, a quarantine command is

not "generate[d]" automatically by the "system," but rather is "manually initiated by a human

administrator." Op. 60; '176 patent at 17:9, 17:29-31, 18:65, 19:17-19; Tr. 1111:25-1112:15

(Dr. Cole admitting that claims require the "system" to "automatically" generate the rule).

Centripetal now contends that "Stealthwatch generates" the quarantine command in step

1 of the diagram from PTX-1089 ("Apply ANC Policy 'Quarantine' to 10.123.1.101"), and the

human administrator must merely "approve" it. Mem. 29-30; PTX-1089 at .1238. But the

language just below the diagram confirms that the human does not merely "approve" the

quarantine; the human *"initiates"* it. *See* PTX-1089 at .1238 ("1. ***User initiates*** from

Stealthwatch assignment of previously configured on ISE ANC Policy for this host to restrict

access to the network for this host."). Moreover, PTX-1089's very next page explains all the

steps that a human administrator ("Adam the Analyst") must follow to issue a quarantine

command, including (1) notice the alert and open a "Host Report" to investigate Stealthwatch's

data about that host; (2) decide whether to limit the host's access to the network via a quarantine

command ("ISE ANC"); (3) review whether ISE or any third-party system already assigned an

"ANC Policy" to the host; and (4) "open[] ANC options available for the host and select ISE and

ANC Policy appropriate for assignment," which causes Stealthwatch to send ISE an assignment

request to classify the host with the intended ANC Policy. PTX-1089 at .1239; Tr. 2183:25-

2188:5, 2262:22-2263:10, 2265:24-2268:11. PTX-595 (cited at Mem. 30) similarly explains that

the human administrator must navigate to a "Host Summary" pane and click "Edit" next to "ISE

ANC Policy" in order "[t]o apply an ANC policy to a host." PTX-595 at 179-180. The Court

was therefore correct in finding that, even if a quarantine command could be considered a "rule,"

it is "generate[d]" not by the "system," but by a human administrator.

To the extent Centripetal is suggesting that the "rule" could be embedded software that

merely provides the capability for a user to issue a quarantine command, that would (yet again)

29

be an entirely new theory that Centripetal forfeited by failing to seek leave to reopen discovery, provide notice for the parties to recall witnesses to present and rebut the new theory, or even mention it in proposed findings of fact or conclusions of law. *See generally* Dkt. 419, 475, 725; *supra* pp. 7-8. And such a theory would be futile for numerous reasons, including because previously embedded software is not "generate[d]" or "provision[ed]" "responsive to correlating"—but rather was embedded before any particular correlation could occur.

Finally, Centripetal's motion fails to address an additional basis for the Court's noninfringement finding: Centripetal failed to prove that a rule generated based on a CTA alert could "identify packets received from the host located in the first network." Op. 60; '176 patent at 17:30-31, 19:18-19. Centripetal's motion does not even mention this "identifying" requirement. And to the extent the alleged rule is the CTA alert, as Dr. Cole testified (Tr. 1112:23-1114:6), such an alert does not "identify" any packets—it merely notifies the human administrator that a host might be malicious. Tr. 2265:2-21.[15]

CONCLUSION

Centripetal's motion should be denied.

---

[15] Once again, Centripetal's request for "an amended judgment finding that Cisco infringes" the '176 patent (Mem. 1) is unwarranted because the Court did not address Cisco's additional noninfringement and invalidity contentions. Op. 61 n.21; Dkt. 737-1 at 10-13(¶¶25-32), 147-153(¶¶322, 325-338); *supra* p. 12.

Respectfully submitted,

Dated: February 21, 2024   CISCO SYSTEMS, INC.

By:_____/s/_____
                                            Of Counsel

Dabney J. Carr, IV, VSB No. 28679
TROUTMAN PEPPER
  HAMILTON SANDERS LLP
P. O. Box 1122
Richmond, Virginia 23218-1122
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
dabney.carr@troutman.com

Charles K. Seyfarth, VSB No. 44530
O'HAGAN MEYER
411 East Franklin Street, Suite 500
Richmond, Virginia 23219
Telephone: (804) 403-7137
Facsimile: (804) 237-0250
cseyfarth@ohaganmeyer.com

Louis N. Jameson (admitted pro hac vice)
Matthew C. Gaudet (admitted pro hac vice)
John R. Gibson, VSB No. 72968
Alice E. Snedeker (admitted pro hac vice)
DUANE MORRIS, LLP
1075 Peachtree Street, N.E., Suite 1700
Atlanta, Georgia 30309-3929
Telephone: (404) 253-6900
Facsimile: (404) 253-6901
wjameson@duanemorris.com
mcgaudet@duanemorris.com
jrgibson@duanemorris.com
aesnedker@duanemorris.com

Joseph A. Powers (admitted pro hac vice)
DUANE MORRIS, LLP
30 South 17th Street
Philadelphia, PA 19103-4196
Telephone: (215) 979-1000
Facsimile: (215) 689-3797
japowers@duanemorris.com

31

John M. Baird, VSB No. 77827
Christopher J. Tyson, VSB No. 81553
DUANE MORRIS, LLP
505 9th Street, N.W., Suite 1000
Washington, DC 20004-2166
Telephone: (202) 776-7851
Facsimile: (202) 478-2620
cjtyson@duanemorris.com

Attorneys for Defendant
Cisco Systems, Inc.